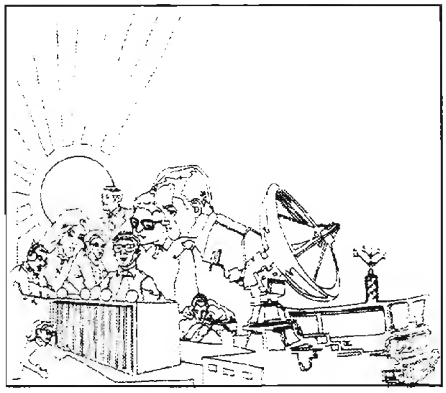
18 APR 1964



NATIONAL SECURITY AGENCY

# CRYPTOLOG

***This Issue:***

# CRYPTOLOG

Vol. XX No. 1 ..... 1st Issue 1994

*Published by P05, Operations Directorate Intelligence Staff*

Publisher .....

P.L. 86-36

Editor ..... (963-7595)

Collection ..... Marian Brown (963-1197)
Cryptanalysis ..... (963-1461)
Cryptolinguistics ..... (963-4382)
Information Resources ..... (963-3258)
Information Science ..... (963-3456)
Information Security ..... (968-8013)
Intelligence Community ..... (963-5800)
Language ..... (963-3057)
Linguistics ..... (963-4814)
Mathematics ..... (963-3709)
Puzzles ..... (963-1461)
Research and Engineering ..... (961-8362)
Science and Technology ..... (963-3544)
Special Research ..... Vera R. Filby (968-6558)
Traffic Analysis ..... (963-3369)

Classification Officer ..... (963-5463)
Unix Support ..... (963-3369)
Macintosh Support ..... (961-8362)
..... (963-4382)



To submit articles and letters, please see last page

# Table of Contents

CRYPTOLOG
March 1994

# The Director's Summer Program



R51
R51

*~~(C)~~ Mathematics is the fundamental science that supports the twin disciplines of cryptology: the design of encipherment systems, and cryptanalysis, the "breaking" of codes intended to be unbreakable. The ever-increasing mathematical sophistication of cryptographers and cryptanalysts outside NSA, the increasing number of important cryptologic problems, and the increasing complexities posed by modern modems and communications systems requires us, more than ever, to bring the newest and most powerful ideas in mathematics to bear on our problems.*

*(U) For the past four summers, the R51-sponsored Director's Summer Program (DSP) has invited exceptionally talented young mathematicians from across the nation to NSA for up to 12 weeks and exposed them to the excitement of cryptologic mathematics by giving them hands-on experience working on some of our most difficult and important cryptologic problems under the direction of top Agency mathematicians. The program has been enormously successful in its first four years (1990-1993), obtaining surprisingly effective operational solutions to very hard problems, encouraging participants to continue their study of mathematics, and helping NSA to become better known in the active network of outstanding young mathematicians.*

*(U) Entry into this program ideally will take place between the junior and senior undergraduate years, but exceptional older or younger undergraduates and high school students may be considered.*

## DSP's Beginning: 1990

(U) Even before the evidence of decline in mathematics research and education was so prominent on the front pages, NSA mathematicians were aware of it and were trying to do something about it through a number of grass-roots efforts. With the austerity we face, we are not going to be able to survive beyond the nineties with business as usual. We are going to have to scour the nation for the best mathematicians we can find. In October 1989 the Agency began an energetic program to seek out top young undergraduates who showed great promise and interest in mathematics and expose them to our exciting problems. Many thought we were doing this as a long-term recruiting program. Indeed, we were recruiting, but for mathematics, not for NSA. Our interest and intent was to use a summer experience with us, to generate evidence that mathematics provides both subject matter and training for challenging careers. We had hoped for a few more students, but we were pleased that eight were able to stick it out through the processing and come, because they were eight very special young people.

(U) We were hoping that we could put these eight young people in a room by themselves, working on our best problems, so that the experience would be strongly peer-interactive. But such an aggressively structured experience could be pulled off only if our top mathematicians took on responsibility for technical direction. The first two mathematicians that we asked to lead the 12-week 1990 DSP not only said yes, but they worked hard during the spring to prepare for the students, identifying and developing the best problems to present to them.

(U) The first two weeks of the 1990 DSP were extremely difficult, for both the technical directors and the students. The students had to learn decades of classified cryptologic mathematics in two weeks, as well as a myriad of details about the four problems presented to them. During these two weeks, some learned to program for the first time. All were proficient programmers by the end of the summer.

(U) By the third week, the students knew everything there was to know about the problems, had developed into overlapping groups, and knew NSA slang and jargon so well they sounded as if they had worked for us for 10 years. We had five Sun terminals connected to the Cray in the room for the eight students and two technical directors, but we had to add three more terminals. The students made substantial contributions to all the problems they worked on and even came up with innovative ways of looking at our problems.

(U) On the fifth and tenth weeks, the DSP students obtained very important results by substantially solving two of the problems, convincing the last of the skeptics that this program was very worthwhile. The real payoff was not the contribution to our product, impressive as those contributions were; the real payoff was the pipeline. Incredibly, before they met us, two of our DSP students, juniors, had not been planning to go on to graduate school following their senior year. These two were performing exceptionally well in their current, demanding academic programs and, ironically, made the most direct contributions to the most significant results of the workshop. One went home from the DSP with a surge of confidence, applied to all the top graduate schools and is now in a Ph.D. program on a fellowship. The other wished to become an NSA employee, but we talked her out of joining us right away. She took all pure mathematics courses her senior year and is now in graduate school in a Ph.D. program on a fellowship.

EO 1.4.(c)
P.L. 86-36

## DSP 1991

~~(C)~~ The 1991 DSP was also very successful. With the 1990 success, it was easy to recruit three top technical directors. They led a larger group of participants, including some 1990 returnees, to complete solutions of three problems and significant results on four others. We had 20 Sun terminals for both the technical directors and for this group of 13 bright young mathematics students, which included two graduate students, four beginning graduate students, three seniors, two juniors, and two sophomores. Eight problems were chosen, from Z, C6, R2 and W and presented to the students. By and large, the problems were quite difficult. Nevertheless, significant progress was made on several of them.

[redacted]

~~(TSC)~~ Success was also achieved on the COMSEC problem [redacted] In addition, important progress was made on the W problem. All but one of the submitted problems were addressed and two or three additional short problems were introduced.

~~(C)~~ Three technical directors and three problem supporters were on hand for the 1991 session. The participation of these agency mathematicians was crucial to the program's success. An overview of 30 years of cryptologic mathematics was distilled into the first two and one-half weeks. Concurrent with these introductory talks on the problems and certain topics in cryptanalysis, the students selected a problem or problems (most settled on one or two) and worked individually, or together, or with one of the NSA mathematicians towards a solution.

(U) A series of Wednesday "progress reports" was held in which students would present work in progress, partial solutions, difficulties encountered, etc. These talks were attended by interested personnel from around the Agency. It was found that these progress reports were valuable to the technical directors, technical support personnel, outside listeners, and students alike.

[redacted]

(U) At the end of the 1991 DSP session, some of the students gave talks on their work to audiences in Z, C6, and R51. Three of the students wrote R51 mathematics papers on their work. In October 1991, [redacted] Chief R51, briefed the final report on the DSP for 1990 and 1991 to the Director NSA.

(U) We can say without reservation that every one of the thirteen students of the 1991 DSP left NSA a better mathematician than when he or she arrived. Each developed a perspective of how mathematics can be used to create and destroy, to win and lose, and to succeed and fail. They saw how their country needs their skills and they came to appreciate how these same skills can be used as a potent weapon against their country.

## DSP 1992

(U) The 1992 DSP session clearly eclipsed the success of the previous two summers in terms of attracting its most talented group of young mathematicians and solving cryptologic mathematics problems. We had an exciting set of top-notch applicants for the 1992 DSP. This can be attributed to the NSA recruiting process which has helped to generate a very impressive group of more high-caliber students than in previous years. Thus, this third annual DSP brought together 16 matchless mathematics students for the 12-week session which commenced on 3 June 1992. Three technical directors provided full-time mathematical support, and 21 Sun terminals were used in this year. Of the 16 DSP participants, 13 were first-timers and 3 were returnees.

~~(S-CCO)~~ As before, the first one and one-half weeks consisted of cryptanalytic orientation and workshops, comprehensive programming in C, and lectures on classified mathematical techniques. The week of 15 June focused on problem presentations. Eight difficult problems were chosen from Z, W, C61, R21 and R51.

[redacted]

(U) For the latter, the team working on Golomb's Conjecture successfully programmed a sophisticated algorithm for generating all sequences with the desired properties and tested the conjecture on the output. Their results will appear in an outside technical journal.

EO 1.4.(c)
P.L. 86-36

## DSP 1993

~~(C)~~ The group of 17 new students gathered for the 1993 DSP set a new standard which will be difficult to exceed. Nine problems were presented to the group and all but one received attention. The group met in a new room in the R&E building which was especially designed for the DSP. Each student and each of the four technical directors had a SUN work station tied in to a CRAY computer. The room is large with ample blackboard space for lectures and discussions.

EO 1.4.(c)
P.L. 86-36

~~(TSC)~~ The summer started with the usual course on cryptologic mathematics and the presentation of the problems. Once the students settled down to work there was no stopping them. The first solution came in the

[redacted]

## DSP's Future

~~(C)~~ We hope austerity will not diminish our ability to continue this program and attract outstanding summer employees. The need for brilliant young mathematicians will only increase as cryptology and cryptanalysis become more and more mathematical. We need to cultivate deep roots within the academic mathematics community and establish a network of academic consultants who understand our mission.

(U) All this makes the Director's Summer Program even more important and timely.

# OPEN SYSTEMS: What Does it Really Mean?

[redacted]
*A7 Architecture and Planning Branch*

P.L. 86-36

Ask any dozen people what the term "Open Systems" means and you're likely to get a dozen different answers. Some interpret "open" very literally and presume that they can build an open system by throwing together any mix of commercial products and *voila*! they have one. At the other end of the scale, some equate open systems with particular products and brand names. "Open" is confusing at best because open systems really aren't open at all. A far more accurate expression is "Standards-Based Systems" since open systems are based on open standards, and standards imply restrictions.

For instance, the specification for an electric outlet is an open standard. The availability of such a specification allows any entrepreneur to produce electric outlets for public consumption at a reasonable cost, and allows others to produce components which work in concert with them; most notably electric plugs attached to electric appliances.

The same general definition of open standards applies to the computing world. The most visible example of an open computing standard is the IBM PC hardware specification. When IBM released the PC in the early 1980s, they did something unprecedented (for them at least). They released the hardware specification to the public in order to encourage entrepreneurs to develop products for their microcomputers. The result was a revolution that spawned an entire industry and made desktop computers as familiar to the average American as a television set.

Another prominent example of an open computing standard is the X/Windows specification. Developed and refined almost completely in an academic environment, it has had a profound influence on our current view of corporate computing. The X/Windows specification is available from the Massachusetts Institute of Technology (MIT) for the cost of the medium on which it's delivered, or alternately the cost of the phone call required to download it from the Internet.

Open standards, by definition, are supposed to be non-proprietary. This means that no individual or organization holds exclusive rights to specifications adopted as open standards. But the fact that the standards are publicly available doesn't necessarily mean that they are in the public domain. Formal specifications are often protected by copyright, and the product characteristics they define may be protected by patent. Therefore, the existence of an open standard doesn't always imply that you can get it and use it for nothing. Access to the specification and its subsequent use may be contingent on payment of a license fee or royalty of some sort. Note there is nothing in the DoD or NSA open systems standards documentation that states that all open standards specifications are to be available at no cost.

To recap: first of all, when we use the term "Open Systems" we're really referring to standards-based systems. Those systems are based on "open standards" which are available to the general public, but their use may have some strings attached such as royalties or license fees. With that understood, we can move on to the real issue, which is:

### *What "Open Systems" means to the typical NSA employee*

- To computer users, it means more robust software with a consistent "look and feel," more effective ADP support, and more rapid delivery of essential capabilities and services at lower overall cost.

- To acquisition planners and managers, it means that at long last there are consistent metrics by which proposed hardware and software acquisitions can be evaluated for "goodness of fit" in the NSA computing environment

- To computer system developers, it means that there will be a stable, predictable, and consistent hardware, software and communications baseline available to them because everyone is playing by the same rules. The most obvious benefits to be realized by developers in such an environment are: vastly improved opportunities for software component re-use, significantly reduced development time, and dramatically reduced support costs. It also opens the door to effective sharing of resources across organizational boundaries.

**Our computer users are the big winners** because, by conforming to a globally accepted set of specifications for hardware, software, and communications (i.e., open systems standards), it's far more likely that any given application will have to be written only once with full confidence that it can be easily moved to any other platform which provides the same specified services and interfaces. Not only that, but also many of the formerly "error-prone" parts of software development, like programming for communications and graphics, can be minimized through re-use of highly reliable "canned" components. Since such functions are fundamentally the same on every computer because of inherent portability, users will be able to move from one conforming system to another (even on a different vendor's hardware) and perform the same without culture shock or retraining.

Obviously, it's important during the process of selecting components for new systems to be able to stick exclusively with products which conform to the standards. However, it's more important to understand not only the basic character, but the limitations of the standards as well, because there are very few standards-based products on the market which reflect a one-for-one mapping of standards specifications to features. Vendors make their standards-based products desirable by adding attractive bells and whistles which make their products easier to use or more powerful than their competitors'. It's these value-added features which sometimes tend to lock us into specific vendors and eventually make interoperability and portability of applications difficult. Knowledge of the standards allows computer system developers to avoid product features which jeopardize portability and interoperability, or allows them to at least associate some degree of risk with those features should a decision be made to take advantage of them in an operational application. Caveat emptor!

In summary, "Open Systems" is simply another way of referring to standards-based systems. ***It is essential to remember that standards are specifications and not products.*** It is equally important to remember that standards do not carry the force of law. Rather, they are guidelines to be followed. If the standards inhibit getting the mission accomplished or blow the budget, the non-standard specifications are the correct choice.

The rewards for following Open Systems Standards will be a significant improvement in the way we design, develop, and support systems, more productive users, and reduced cost at every step of the acquisition and support cycle. The NSA standards baseline is the NSA Open Systems Standards Profile, which is an adaptation of DoD's standards—the Center for Information Management's Technical Reference Model (CIM TRM).

The success of the whole open-systems venture depends on the willingness of vendors and developers to build products which conform as closely to the standards as possible. It also depends on the willingness of acquisition officials, from division level on up to the key components, to support the purchase of those products which conform to standards, with full awareness that doing so may sometimes mean sacrificing power and convenience in favor of portability and interoperability.

That, in a nutshell, is a view of Open Systems. Anyone interested in getting a copy of the NSA Open Systems Standards Profile, in learning more about Open Systems at NSA, or becoming actively involved in the Open Systems implementation process should contact [redacted] the chairman of the NSA Open Systems Working Group. Ken can provide information on DoD and industry standards efforts and can point you toward sources of information and working groups already involved in formalizing an NSA Open Systems implementation process. He may be reached via NSA e-mail by sending a message [redacted]

P.L. 86-36

# The CIM TRM and the NSA Profile

[redacted]
A7 Architecture and Planning Branch

P.L. 86-36

***What's in it for NSA? Why are we cooperating with the DoD Corporate Information Management (CIM) Office?***

(U) The CIM TRM (Technical Reference Model) is the statement of its open-systems standards available. It describes the entire open computing environment (i.e. hardware, operating systems, communications, etc.) in terms of standards. The intent is to create a set of standards that DoD can use to increase its buying power, decrease the cost of what it buys, and give DoD more of a voice in the development of future computer products. NSA is working on adapting the CIM TRM to meet NSA's needs, not because of a DoD requirement, but based on our self-interested desire for a framework of specific standards which will let us buy hardware, software, and integrated systems that will work together with a minimum of tinkering and that will continue to work together without constant pampering. The NSA adaptation of the TRM is known as the NSA Open Systems Standards Profile, or "the Profile" for short.

**Why Does NSA Want the Profile?**

~~(C)~~ Over 75 percent of the total cost of any computer system made today is for maintenance. The lion's share of that cost is for support personnel. At NSA today, there is about one identified computer support person for every 8-10 computers. However, that ratio is understated. There are a lot of computer gurus working under non-computer COSCs who spend most of their time doing computer support tasks. With NSA being told every year to justify its budget using ever more restrictive criteria, this has to change. What is needed is a strategy which reduces the support tail. Adoption of a standards-based architecture can provide the foundation for such a strategy.

(U) The purpose of the NSA Standards Profile is to provide the guidelines for that standards-based architecture. Rather than a list of "must do" actions and "must use" products, it talks about what the standards are, which ones are currently fully enough developed to be widely and most easily used and which ones we are looking at for the future. The Profile also talks about our legacy systems. While those systems have served well, they do not and often can not support our need to move toward an open systems environment.

(U) An open standard is based on widely recognized and used specifications which are in the process of being made into formal standards, or which have already been formally adopted as standards by groups like the American National Standards Institute (ANSI) or the International Standards Organization (ISO) and catalogued by the National Institute for Standards and Technologies (NIST).

(U) Through judicious application of appropriate standards, the Agency hopes to improve:

- ***user productivity*** with a consistent user interface, intelligent integration of applications, corporate data sharing, and consistent security control;
- ***developer efficiency*** with more common development efforts for problems, providing a standards-based information-processing environment The best way to improve developers' efficiency is with the use of Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS) software, setting up mechanisms for component reuse and resource sharing;
- ***application portability*** from one type of computer to another and scalability (from one size task to another) through attention to standards and a deliberate effort to address the largest number of computers possible;
- ***opportunities for interoperability*** of systems and applications through a common, standards-based communications and computing infrastructure and common services; and
- ***manageability of systems and resources*** by simplifying development and acquisition processes.

(U) At the same time NSA wants to reduce:

- ***dependence on vendors*** by acquiring or developing interchangeable, non-proprietary software;
- ***life-cycle support costs*** by eliminating duplicate development efforts, improving maintainability, and improving training.

**What Needs to be Done?**

(U) Agency seniors personally supported and directed the Profile's development by creating an all-seniors NSA Open Systems Steering Group (NOSSG). In turn, the NOSSG selected mission-critical ADP personnel to chair and staff the NSA Open Systems Working Group (NOSWG). Subgroups consisting of experts from all relevant key components were then formed:

**Programming Services** classified existing and proposed programming languages according to their conformance to ANSI, ISO, and POSIX standards.

**User Interface Services** standards describe how a user will interact with a computer's programs, especially the graphical display of information. NSA will use the X Window standard and the DoD Human-Computer Interface Style Guide.

**Data Management Services:** standards, for database designers mostly, describe how data will be stored, accessed, modified and loaded.

**Data Interchange Services:** another set of standards mainly for database designers, dealing with data exchange formats, from software package to software package.

**Multimedia Standards:** deal with how multiple types of information (text, audio, pictorial, tactical, etc.) will be presented, edited, or integrated.

**Network Services:** how computer hardware and related communications nets will work together to deliver information and operate.

**Operating System:** the basic package of instructions that turns a delicately carved piece of sand into a device that can process information. NSA has selected POSIX as its future standard operating system.

**Security Services:** interacts with all the other standards to insure that data will be accessible only to authorized individuals, and that data will not be maliciously or accidentally destroyed or corrupted.

**Management Services:** for software tools used to keep software, hardware and network communications systems working and productive.

**Real-Time Services:** for systems that need to collect, process, or evaluate information as it is occurring;

(U) Next, an implementation mechanism was built for the Profile. The NSA Open Systems Standards Profile will be implemented by a transition plan prepared as an accompaniment to the profile. It provides a road map for getting from where we are today in terms of our computer capabilities to where we expect we will need to be in the future. This means the plan will provide for compatibility testing and information dissemination; create a mechanism for projecting future requirements; and for investigating new standards and products to satisfy future needs.

(U) Creating a way of discussing and classifying existing standards took a lot of time. But this classification system will allow developers and managers to understand how much risk they are taking when selecting standards for a project and the various products that use that standard. The Profile does this by breaking standards into six levels:

1. Now: a product conforming to this standard can be freely used. The investment risk of using a product meeting this standard is minimal.

2. Now: a product conforming to this standard can be used with prior approval. The investment and risk of using a product meeting this standard must be considered. Also, the standard may not be in line with established guidance.

3. Future: a product conforming with a proposed standard can be used with prior approval. The standard is still moving toward approval, can still change unpredictably, and so long term investment risk exists.

4. Gap: no recognized standards exist for this capability or product availability is limited. The risk of using such a product is moderate to high and requires prior approval.

5. Void: while NSA hopes standards will emerge in the future, none have yet. The risk of using such a product is extremely high. Since products in this area have no standard, their use is discouraged.

6. TBD: a standard has been proposed, but either has not begun evaluation or is in the early stages of being evaluated. Since very substantial changes can occur, the risk level is high and prior approval is recommended.

**How Will the Profile Affect You?**

~~(FOUO)~~ Some groups will benefit immediately, while other groups will see no changes or benefits. However, over time (at a guess, five to ten years) everyone stands to benefit. Examples are: the Agency needs to constantly update the computers we use and the [redacted] communications system.

[redacted]

~~(C)~~ [redacted] The solution to these concerns that the Profile encourages is to decrease the cost of our equipment purchases by adhering to DoD and government-wide standards while using our software-development resources for problems that need to be solved on a custom or time-critical basis. This benefits analysts by freeing up more programmers to perform software work for them. Computer professionals will benefit by having more time for developing software for analysts and needing to spend less time maintaining existing systems.

~~(C)~~ [redacted] initially benefited no one. It tied almost no one to almost nothing. But it has since become invaluable. It delivers information electronically, ending the drudgery of sorting out the mail twice a day. Also, you can now send e-mail to a person instead of spending days playing "telephone tag."

(U) The NSA Open Systems Standards Profile is designed to be a living document providing advice—not guidance—about open standards rather than products. It is intended to be periodically updated as the technology changes. It is NSA's response to the challenge not just of the DoD's CIM—but more important, to the changes that are accelerating as the Information Age finally moves beyond its barest beginnings. ***Within fifteen years NSA must either adapt to that age's requirements or die.*** The adaptation process will require a wholesale reinvention of NSA; the Profile will be one of the guideposts of that process.

(U) Information on the Agency's open systems efforts is available in NetNews under the heading of org.noswg. This contains the minutes of NOSWG meetings, and NOSWG subgroup meeting notes and working drafts.

CRYPTOLOG
March 1994

# The Closing of NSGA Philippines

P.L. 86-36

[redacted] USN

*This article is dedicated to all those persons who perished as a result of the eruption of Mount Pinatubo Volcano.*

It began in February 1991. A volcano which had remained dormant for over 600 years was now showing signs of coming back to life again. Although no one could have foreseen the extent to which Mother Nature's fury would be cast upon the Republic of the Philippines in the months to follow, it began with a series of what seemed to be innocuous ventings of steam from the depths below. By early March 1991, enough venting had occurred to warrant some professional investigation and analysis. Several volcanologists and seismologists arrived on island to determine the extent of the activity. There, scientific readings and measurements told them that the mountain was capable of erupting within twelve months.

With this information, Clark AB, located approximately 9 miles from the volcano, soon began publishing information in order to prepare the base for a possible evacuation. A plan was quickly put together by on 6 June 1991, when the eruption of Mount Pinatubo was almost a reality.

While each tenant command aboard Clark AB passed on the seismological information to its people, NSGA Philippines had been working more diligently on a different approach. Specifically, a plan to close down the command, which had been drafted some twelve months earlier in the event the base negotiations with the Philippine government were unsuccessful, had been dusted off and examined. The plan essentially listed all those actions necessary to close and disestablish a command. Its 180-day timeline was merely modified into separate 3-day, 7-day and 30-day action processes, depending entirely upon Mother Nature's cooperation, of course.

As I recall, on 9 June 1991 word had quickly spread that the mountain could blow within a matter of days. It was venting more, and the color of the steam had changed from a pure white to grey within the past few days. Venting could now be seen from different sections of the mountain as well.

At 1700 hours on 9 June 1991, an emergency recall of NSGA Philippines was ordered. All leave was cancelled. The skipper briefed us on the latest scientific findings, which concluded that there was a good chance the volcano would erupt within 48 hours, and that a decision to evacuate Clark AB could come as early as 0500 the next morning. The theme was "don't panic but be prepared to go." Earlier that week a list of items that should be readied in case of an evacuation was provided to each person and family as well as being posted throughout the command. Also during the previous week, information concerning lodging, transportation, food, and a host of other items was similarly disseminated.

With 100 percent of the command recalled, a Phase I (precautionary emergency destruction) was ordered by the Commanding Officer and passed on to the CDO to carry out. For several hours and until almost midnight on 9 June, we destroyed as much classified information as we could. What had been an otherwise quiet weekend within the operational spaces of NSGA had turned into a command-wide emergency destruction operation within a matter of hours. What we could not destroy under Phase I, and all Phase II and III material, was boxed up, double-wrapped, and would eventually be couriered to Subic Bay Naval Station, which was designated as the evacuation safe-haven site; we intended to return to Clark after the eruption.

At 0500 on 10 June, the order to evacuate Clark AB came. All personnel, less a five-man closure team, mustered on the flight line as previously instructed. Within a few hours, a convoy of some 25,000 military, civilian and dependent personnel were on their way to Subic Bay, some 35-40 miles away. The trip lasted approximately five hours, and everyone arrived safely. The five-man closure team from NSGA Philippines remained behind to continue the destruction of classified material and the powering down of electronic equipment.

Without lights and with flashlights in hand we continued to check each safe, desk, and cabinet for classified material. What little we did find, we destroyed. However, owing to the sheer volume of paper products in the building, it was clear that a 100-percent sanitization certification could not be given unless all paper products were destroyed.

## The First Eruption

On 12 June 1991 at 0700 the five of us who constituted the closure team once again departed the barracks for the Operations Building to continue our search for classified material. Armed with our flashlights and radios, we continued the search. At 0848, however, a call from Alpha Alpha (the CO) was received. *"This is Alpha Alpha, major eruption, get out of the building."* Instinctively, I began to stuff the burn-bags back into the safe and had planned on securing the safe. This took approximately 45 seconds. My second thought was to call Subic Bay and advise them the eruption had occurred and that we were evacuating. By this time a second call from the radio was heard: *"Major eruption, get out of the building NOW!!"* Not knowing the extent of the "eruption" and whether or not the pyroclastic flow would reach the base (which reportedly travelled at a rate of 125 miles per hour), nor what I would find once I got outside of the building, I was determined to notify NSGD Subic before I exited the building.

After I secured the material, I ran, flashlight in hand to one of only two phones working in the Operations Building. The building was completely dark and smelled of must. By this time, approximately one to one and a half minutes elapsed since the first radio call from Alpha Alpha. Just as I began to dial Subic's telephone number, I received (in a much more direct tone) another call from Alpha Alpha, which meant that if I knew what was good for me, I would get out of the building now. I did just that.

Upon running out of the Operations Building, I looked to my starboard side. I was in awe! What had for months been a steam venting "hill" had transformed itself into a monstrous grey plume rising 88,000 feet. It looked exactly like a nuclear detonation. The surprising thing was that it made no noise at all.

I reached the vehicle parked outside the gate where the skipper and the other three were waiting, motioning me to hurry. We departed for the barracks approximately 1/4 mile away to pick up our bags. With sirens blaring we retrieved our "go bags" and headed to the flight line (the primary evacuation point). Upon arriving at the flight line about 10 minutes later, we saw the plume, which at one point appeared to be overtaking the base, now seemed to be retreating in the opposite direction, owing to a shift in the wind. In any case, an order to proceed to the secondary evacuation point was given and we drove through town approximately 10 miles to Mount Arayat. There we waited approximately five hours before receiving the all-clear sign where we returned to Clark AB. As I found out later, we evacuated to Mount Arayat because of the uncertainty of the pyroclastic flow.

The skipper didn't go to Mount Arayat; he and Lt. Col. Hurst, Commander of the USAF ESS element at Clark AB, remained on the base. We eventually met up with him when he decided to leave Clark and proceed to Subic. It was just too dangerous to stay. So at 1800 hours on 12 June 1991, the five of us departed Clark AB for what we thought to be the last time.

We arrived in Subic Bay at 2145 that evening, met by the OIC, XO (Lt. Cdr. Keith Ludwig) and the CDO. Berthing arrangements were made in advance and we called it quits for the evening.

The next two days were spent trying to keep a 137-man organization and its detachment of approximately 50 sailors together, fed, and informed. Additionally, destruction of the classified material transported from Clark to Subic continued. This time, however, the Commanding Officer ordered a full emergency destruction of all Phase I, II, and III material. His rationale, I believe, was that after having personally seen the eruption just a few days ago, it was important to destroy as much as we could while we still had the chance. After all, it would be easier to ask for another copy of this or that, than to justify what we lost, why we lost it and the extent of compromise. His decision was certainly the correct one under the circumstances.

The emergency destruction of Phase II and III material took about 18 hours. Dumpsters were made into infernos, shredders were used around the clock. Axes and sledgehammers were used for the disk-packs and equipment. Of course, accounting for the items destroyed was important. During the entire period, a strict accounting of all of the items destroyed was maintained. The resultant 92-page destruction report containing 5500 line items was an achievement in itself, considering the circumstances under which the destruction and reporting took place. There was no power (we had portable generators hooked up outside of the building, one or two of which belonged to personnel from the detachment); we had been eating MREs for the past three days; there was little or no potable water (we flushed the commodes with sea water); and we were in the midst of a non-combatant evacuation (NEO) of all civilian and dependent personnel to the island of Cebu for transportation to the United States. Needless to say, there was a lot going on at one time.

### The Major Eruption

We continued the destruction of classified material and tried to organize the two commands (NSGA/NSGD) into one cohesive unit as best we could. But on 15 June, all that changed. At approximately 1000 Mount Pinatubo erupted again. This time the plume reportedly reached 120,000 feet or so. But this time we were all located at Subic Bay, well out of danger zone, or so we had been told.

The very instant the mountain erupted that second time, Typhoon Yuna (or Yuma, I can't recall) happened to blow our way. As a result of that eruption, a plume of 120,000 feet of ash blown by the winds of the typhoon not only blanketed Clark AB, but wiped out Subic Bay Naval Station, covering it with 10-12 inches of ash fallout. The sheer weight of ash mixed with water toppled buildings left and right. Approximately 30-40% of Subic Bay's building structures had collapsed. Moreover, the magnitude of the eruption was so great that it put much of the Philippines in total darkness for over 28 hours. It reminded me of a New England blizzard, except for its color (destructive grey) and the surrounding temperature (90 degrees).

"Gainfully employing" members of both NSGA and NSGD had new meaning now. Shoveling crews were assembled and dispatched to various locations and buildings to remove the fallen ash to prevent further damage and collapse. Roads were plowed, sidewalks cleared and power lines hosed off. Within approximately 10 days, Subic Bay was operationally restored.

For the next few weeks, plans were made to close down NSGA Philippines and transfer its people to other bases. Upon receipt of the go-ahead, PCS orders began arriving via fax and within three weeks, the admin crew had completed all transfer evaluations, fitness reports, medical screenings and all of the other associated paperwork which normally accompanies a PCS transfer. By the end of July approximately 85% of the command had transferred. It was a remarkable achievement administratively, and a testament to the professionalism displayed by the admin crew.

The remaining weeks were largely spent deinstalling, inventorying and shipping over $15 million worth of sensitive electronic equipment from the Operations Building at Clark AB to Subic Bay for transfer to the U.S. Additionally, the closure team, assisted by members of the detachment, ensured that all NSGA members' personal property (each household and barracks room) and POVs were packed and shipped.

On 1 September 1991 at Cubi Point, a brief change of command ceremony was held between CDR Bernas and LT Wickham. Lt. Wickham, now officially the Commanding Officer, had bidden farewell to the remaining few as we boarded Hawaiian Air for home.

To say the least, it was an eventful eight-month tour. I did however enjoy those months and have learned many things as a result of them. I will especially miss the people of the Philippines and the food. And I will always remember the team work which was displayed by the sailors of NSGA Clark and NSGD Subic. It was teamwork which kept us going and brought us through 90 days of frustration, danger, and uncertainty.

To all of you, Godspeed.

ACKNOWLEDGMENTS

*Special thanks are due to:*

*CDR Barry L. Bernas, USN, Commanding Officer, U.S. Naval Security Group Activity, Clark AB, Republic of the Philippines;*

*LT Kenneth Wickham, USN, Officer-in-Charge, U.S. Naval Security Group Detachment, Subic Bay, whose staunch leadership and concern for the safety of the crew prior to and after the emergency were truly inspirational.*

CRYPTOLOG
March 1994



# EUROCRYPT '92

(U) Eurocrypt '92 continued the string of successful congresses sponsored by the IACR (International Association for Cryptologic Research). For the first time, the meeting was hosted by an Eastern (Central?) European country: the venue was Balatonfüred, Hungary; the dates, 24-28 May 1993.

(U) Attendance was announced as 253, but a preliminary registration list which was circulated contained only 240 names. From that preliminary list, we have the following accounting, by home address, of the registrants:

| | |
|---|---|
| Germany | 42 |
| U.S.A. | 30 |
| France | 27 |
| Hungary | 15 |
| Great Britain | 14 |
| Sweden | 14 |
| Italy | 12 |
| Austria | 10 |
| Switzerland | 10 |
| Netherlands | 8 |
| Denmark | 7 |
| Japan | 7 |
| South Africa | 5 |
| Spain | 4 |
| Belgium | 4 |
| Norway | 4 |
| South Korea | 4 |
| Canada | 3 |
| Romania | 3 |
| P.R. China | 3 |
| Israel | 2 |
| Australia | 2 |
| Yugoslavia | 2 |
| Czechoslovakia | 2 |
| Singapore | 2 |
| Saudi Arabia | 1 |
| Egypt | 1 |
| Finland | 1 |
| Ireland | 1 |

(U) There were some prominent "cryptologists" who did not attend: Adi Shamir of Israel (we've heard that he may by preparing a book, probably containing his work on "differential cryptanalysis"); Ron Rivest and Silvio Micali of MIT; Canada's Claude Crépeau and Gilles Brassard; Gus Simmons of Sandia; Agnes Chan of Northeastern; David Chaum of CWI, Amsterdam; Louis Guillou of France, and Ivan Dåmgard of Denmark. All of these have been more or less regular attnedants at previous IACR meetings. Three world-class mathematicians attended: Arjen Lenstra of Bellcore, Harald Niederreiter of Austria, and Andrew Odlyzko of Bell Labs.

(U) The General Chairman was Tibor Nemetz of the Mathematics Institute, Hungarian Academy of Sciences. I understand that some people experienced difficulties with bus connections, but I personally had no problems. As usual, I did not participate in any of the scheduled social activities, even eschewing the communal lunches and dinners. This policy is probably an error, and in the future I may try a more friendly posture.

(U) Rainer Rueppel, the excellent Swiss (formerly with Crypto AG) who is operating a free-lance consulting business, chaired the Program Committee, which included some of the best researchers in the community: Kevin McCurley (Sandia), Yvo Desmedt (University of Wisconsin, Milwaukee), Joan Feigenbaum (Bell Labs), Jovan Golic (University of Belgrade), Tor Helleseth (University of Bergen) Peter Landrock (University of Århus), Tatsuaki Okamoto (NTT Labs), Jennifer Seberry (University of New South Wales, Australia), Othmar Staffelbach (Gretag), Jacques Stern (ENS-DMI), and István Vajda (University of Budapest.)

(U) Of the 88 papers submitted, 54 were evaluated favorably, but only 35 could be accepted. The leading countries, with their acceptances/submissions, were:

| | |
|---|---|
| USA | 8/14 |
| Germany | 7/13 |
| Japan | 4/12 |
| France | 3/7 |

One was submitted from Russia, two from China. The Program Committee also served as chairmen for the sessions.

(U) The program was (for me) awkwardly scheduled (maybe it was convenient for some Europeans who could drive from home in a morning). In the past there had been a lively informal rump session on Tuesday night, as there was again this year, but in compensation Tuesday afternoon had always been left free. This year the free time was Monday morning (!), and Tuesday afternoon from 4:00 till 6:00 was devoted to a potentially controversial panel discussion on "trapdoor primes and moduli," so there was little respite from the concentrated dosage of research reports. Altogether 34 papers were presented (one cancelled), each allotted 15 to 30 minutes, and the schedule was adhered to fairly strictly (good!). The order of the program, which will be followed in this report, was as follows:

Monday afternoon: secret sharing, hash functions.

Tuesday morning: block ciphers, stream ciphers.

Tuesday afternoon: public key I, factoring, panel discussion.

Wednesday morning: public key II, pseudorandom permutation generators.

Wednesday afternoon: complexity theory and cryptography I, zero-knowledge.

Thursday morning: digital signatures and electronic cash, complexity theory and cryptography II.

(U) Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (this is good news!). The scholarship was actually extremely good; it's just that the directions which external cryptologic researchers have taken are remarkably far from our own lines of interest.

(U) There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. I really don't see how things could have been any better for our purposes. We can hope that the absentee cryptologists stayed away because they had no new ideas, or even that they've taken an interest in other areas of research.

(U) I had thought of offering a representative "theorem" from each of the papers, so you could judge for yourself that the paper was without interest (that is, except to the small number of researchers whose livelihood depends upon being able to publish in that field), but most of them require elaborate definitions of terms or symbols, and that extensive a review is merited in only a few cases.

(U) Also, it should be noted that in some cases authors had, in the time between submitting the preliminary abstract and delivering the talk, significantly improved (or corrected) the presentation. In such cases, the change was usually great enough, and my understanding so poor, that instead of trusting my memory for what was said I shall usually rely on the printed abstract.

(U) The first six papers were on secret sharing (2) and hash functions (4). Alfredo DeSantis (University of Palermo) spoke on "Graph decompositions and secret-sharing schemes," a silly topic which brings joy to combinatorists and yawns to everyone else. Gus Simmons, Doug Stinson, and Marijke de Soete are the big names here, and Stinson is a coauthor of the current work, along with the Italians C. Blundo and U. Vaccaro.

(U) Yvo Desmedt, the "mad Belgian," seems to have caught on at the University of Wisconsin, Milwaukee. He's also been getting respect from the IACR, being on the Program Committee and also on the Board of Directors. As befits a person of honor, he no longer rattles the rafters with his staccato delivery, but his interest to us has not changed. His offering this year was "Classifications of ideal homomorphic threshold schemes over finite Abelian groups." His student Yair Frankel is listed as coauthor.

(U) The session on hash functions was as interesting as any. Marc Girault (SEPT, Caen, France) led off. His coauthors were Henri Gilbert, who has done some good work in the past on FEAL, and Thierry Baritaud, both of CNET, Paris, with "FFT-hashing is not collision-free," a criticism of Claus Schnorr's hash function scheme which had been presented at the rump session of Crypto '91. Unfortunately their work was, as Girault admitted, "essentially the same" as the attack by Daemen, Bosselaers, Govaerts, and Vandewalle given at the rump session of Asiacrypt '91.

(U) But have no sympathy for the much-maligned Professor Schnorr (University of Frankfurt)! In an oft-replayed scenario, he was the next speaker, and presented ("FFT-Hash II: efficient cryptographic hashing") a small revision of his sullied scheme. Perhaps it is beneficial to be attacked, for you can easily augment your publication list by offering a modification.

(U) Jim Massey is a prominent American scholar and educator (he's been at the Swiss Federal Institute of Technology, ETH, for many years, and has produced several of the best young cryptologic researchers) whose most recent doctoral student—he's just completed his degree, but I don't know where he'll go next—Xuejia Lai, presented their joint effort, "Hash functions based on block ciphers." A hash function is a special type of function which collapses long messages

into a compressed representation; one thinks of their application as being in signature or authentication *schemes rather than encryption*: Lai and Massey presented some sound theoretical analysis in the case that the function is constructed by iterating an easily computable function. As usual, all the functions considered are very general; no specific proposal is considered. They conclude that it is not easy to produce hash functions which satisfy the usual security concerns.

(C) One specific hash function which has been proposed is Ron Rivest's MD5 algorithm, which produces a 128-bit output for an input message of arbitrary length. Tom Berson, in a very interesting paper, "Differential cryptanalysis mod-$2^{32}$ with applications to MD5," showed that the popular "differential cryptanalysis" technique, introduced outside by Adi Shamir [redacted] can be applied effectively in this situation. Shamir's method has so far been used only in attacking systems which use addition modulo 2, but Berson showed that it can be adapted to fit the mod-$2^{32}$ addition of MD5. This would not have been a particularly attractive piece of work, but Berson carried out quite a bit of tricky analysis, showing commendable analytic power. Berson is the retiring President of the IACR, but I had no previous knowledge of his technical prowess. His work applies only to a single round of the MD5 process and will probably not cause a revision of the algorithm, as there is no reason to think that consecutive rounds can be attacked simultaneously. In particular, Berson's attack poses no threat to the NIST "secure hash standard," which is based on MD4.

(U) The busy Tuesday began with three talks on block ciphers. The first represented a Mitsubishi attack on the NTT FEAL algorithm. It has become popular to pick on FEAL, and several other attacks have been presented at IACR conferences. This one is again based upon possession of matched plain and cipher, and seems to require quite a bit less than its predecessors. They (Mitsuru Matsui and Atsuhiro Yamagichi, "A new method for a known-plaintext attack on FEAL cipher") claim to be able to solve FEAL-4 with 5 plain texts (and 350 seconds of processing), FEAL-6 with 100 plain texts (and 40 minutes of processing), and FEAL-8 with $2^{15}$ plain texts (but their computer is not large enough to see this through).

(U) Kaisa Nyberg, of the Finnish Defense Forces, now gives a Bonn address (maybe she's at some joint European command). She has been doing good work for several years, and her talk "On the construction of highly nonlinear permutations" was not disappointing. Her interest lies in Fourier spectra of Boolean functions and she is particularly enamored of bent functions. She defined the nonlinearity $N(f)$ of a function $f: F^n \longrightarrow F^m$ to be the minimum (Hamming) distance from $f$ to the set of affine functions—that is, $f$ and any affine function on $F^n$ differ by at least $N(f)$ (and in at least one case differ by exactly $N(f)$) values in their truth-table representation. She was able to compute $N(f)$ for quadratic forms, and she asked if the maximal nonlinearity attained by quadratic functions was indeed maximal for all functions (of course, only the case of odd n is in question). Again, this is not new and exciting work, but she showed considerable technique in her investigations.

(U) An East German, Ralph Wernsdorf (SIT Gesellschaft fur System der Informationstechnik mbH, Grünheide; Mark King said that he had been told by his German friends that this company was composed of ex-Stasi people), presented the talk "The one-round functions of the DES generate the alternating group." This result has no cryptanalytic application, but it serves to answer a question which someone with nothing else to think about might have asked. I think all of us would have been surprised if the result had been otherwise, and indeed all earlier research on this problem had pointed to this answer. Everyone feels that in fact the same result holds true for 16-round DES functions (and this is the question that really merits research), and someone will in the near future prove this, though it may be considerably more daunting technically.

(U) The three-paper session on stream ciphers was shortened when Luke O'Connor (Waterloo) failed to appear to present "Suffix trees and sequence complexity," but from the abstract we can see what he had in mind. He has seen Rainer Rueppel's beautiful work on the linear complexity of a sequence (the length of the shortest linear shift register which will generate the sequence), he is interested in using Kolmogorov complexity to generalized the finite case to a "semi-infinite" analogue, and he attempts to deal with the "complexity" (that is, using *any* function, not necessarily linear). Now the methods one should use in this case are quite different, and he seems to be incorrect on one matter (he "proves" a theorem which says that the expected degree of a random function of $n$ variables is near n/2—I'm no statistician, and I know statisticians can prove wonderful things). He produced a really quite remarkable computer study (I don't see how it could possibly be true, but computer scientists have marvelous powers too) of the spans of functions which generate 100,000 32-bit sequences.

(U) Even if his results are correct (and I have on many occasions been shown how simple these things are to understand), the work is, as viewed by cryptanalytic eyes, typical of much of the best work presented at this conference: it may be good statistics (or mathematics, or computer science, or philosophy) but it is not good cryptanalysis. The methods employed would no doubt make a researcher in the appropriate science quite comfortable, but I tend to find them mystifying.

(U) The O'Connor talk was replaced by a talk which had, strangely, been scheduled to be presented at the rump session! Rafi Heiman (Bellcore), probably an Israeli, talked about "Secure audio teleconferencing: a practical solution." His concern is in permitting conference calls through a central "bridge" without the bridge being able to monitor the conversation. There are clearly a great many problems to be solved, and he was able to give us an actual audio demonstration of how the enciphered speech would sound. I was certainly not impressed, but then I've never tried to do it. Certainly security has not played an important role in his concerns.

(U) The other two talks were authored by Jovan Golic, of the Institute of Applied Mathematics and Electronics, School of Electrical Engineering, University of Belgrade. Golic has been active at other IACR meetings (both at recent Eurocrypts and at Auscrypt) but his work has never inspired me. His presentation was very good, but the collection of abstracts did not include his paper "Correlation via linear sequential circuit approximation of combiners;" instead, there were two copies of "Convergence of a Bayesian iterative error-correction procedure on a noisy shift-register sequence," presented by his much less effective coauthor Miodrag J. Mihajlevic, which provided us with yet a third copy. The first Golic talk concerned combiners with memory, and considered their linear approximations.

(U) Tuesday afternoon began with three talks on public-key systems. The first was given by Birgit Pfitzmann (University of Hildesheim), whose coauthor was Michael Waidner (University of Karlsruhe), "Attacks on protocols for server-aided RSA computation." They are attacking a protocol presented at Crypto '88 by Matsumoto, Kato, and Imai on speeding up secret computations with insecure auxiliary devices. Essentially they envision a smart card which interacts with a much more powerful "server," which is regarded as untrustworthy. The Japanese researchers had concocted an RSA-based scheme, but the Germans have found an attack which puts its security under a shade. We were certainly not interested in the original scheme, but the attack shows a certain amount of analytic ability, and the paper is worth at least casual study.

(U) Another German effort, "Resource requirements for the application of addition chains in modular exponentiation" by Jörg Sauerbrey and Andreas Dietel (Technical University of Munich), really had no cryptologic component, being concerned only with the speed of carrying out modular exponentiation.

(U) The allegation (almost certainly correct) that certain public-key systems might be implemented more securely by using elliptic curves has produced the predictable spate of papers on elliptic curves. We were fortunate to have only two such talks on the current agenda. One ("Public-key cryptosystems with very small key lengths") was by Scott Vanstone (Waterloo), working with his students Greg Harper and Alfred Menezes (the latter spoke very well at last year's Crypto). Though the emphasis was undeniably mathematics rather than cryptology, I thought the material was well presented, and that Vanstone never lost sight of the connection.

(U) The same could not be said of Brandon Dixon's talk "Massively parallel elliptic curve factoring." Dixon (Princeton; his coauthor is Bellcore's Arjen Lenstra) is obviously a very smart guy and a clever computer scientist, but his talk was devoted wholly to describing the implementation of the elliptic curve factorization method on a SIMD (single instruction, multiple data) massively parallel computer. The talk was very stimulating, well organized, and provided a useful update on progress in this area of research, but it contained no cryptology.

(U) I think I have hammered home my point often enough that I shall regard it as proved (by emphatic enunciation): the tendency at IACR meetings is for academic scientists (mathematicians, computer scientists, engineers, and philosophers masquerading as theoretical computer scientists) to present commendable research papers (in their own areas) which might affect cryptology at some future time or (more likely) in some other world. Naturally this is not anathema to us.

(U) The most interesting part of the 1992 Eurocrypt was the panel discussion on "trapdoor primes and moduli." Let us set the stage for the uninformed. One of the most critical issues facing the international cryptologic community (and also NSA) is the establishment of universal standards for various cryptologic needs. International trade and banking people, especially, are clamoring for a security system which they may use as though it were secure (they care very little about secu-

rity, of course, but very much about adverse lawsuits). The American NIST, which sets our policy on these matters, needs to consider a great number of issues in setting standards (it seems that everyone else expects American recommendation to become the international standard). NIST has recently announced its endorsement of (a variant of) El Gamal's public-key system for the "digital signature standard."

(C) This decision has been vigorously criticized by the RSA company, which had hoped to realize an enormous profit from the (American) patent it holds on the popular "RSA" algorithm. Of course, while throughout we refer to the extremely popular algorithm as "RSA," it was in fact first conceived by GCHQ's Cliff Cocks, following the introduction of "nonsecret encryption" ideas (Note: now known as "public-key cryptosystems") by James Ellis, also of GCHQ. This poorly kept secret has never been acknowledged publicly, and is still CONFIDENTIAL.

(U) NIST came under fire immediately, and its position became even less comfortable when the eminent number theorist Arjen Lenstra (Bellcore) demonstrated that some the choices of parameters for the proposed system would be unexpectedly weak. Lenstra apparently submitted a paper to Eurocrypt, but the Program Committee decided that the issue deserved more careful attention, so they convened a panel discussion, which proved to be an exceptionally wise decision. It was also thought that Eurocrypt was an appropriate venue for discussion, as the debate in America has acquired a certain amount of rancor.

(U) The panelists were a varied lot. Arjen Lenstra and Andrew Odlyzko are mathematicians of the highest order. Rainer Rueppel and Kevin McCurley are excellent cryptomathematicians. Miles Smid, a former NSA employee (many years ago) now with NIST, lacks the technical ability of the others but is, of course, the most familiar with the issues and their relative importance. Peter Landrock is a capable mathematician, the new president of the IACR, and Yvo Desmedt has published a number of papers. Lenstra is Dutch, Desmedt Belgian, Rueppel Swiss, Landrock Danish, Odlyzko Polish-American, and McCurley and Smid are Americans.

(U) The panel concluded that the RSA's ardent objections were based almost exclusively on financial grounds, and were therefore without merit. They discussed the two systems and found little to choose between them. Everyone knew that the patent difficulty (which applies only in the United States) had influenced NIST's decision, but no panelist quarrelled with the choice. They all agreed that the difficulty which Lenstra had found was extremely subtle (so is unlikely to have been intentionally designed) and would be most unlikely to occur by chance.

(U) Rueppel, playing the "neutral Swiss" role, sketched the many interest groups which needed to be considered, and described the algorithm which had been selected. Lenstra detailed the threats to security, and emphasized the ease with which a clever programmer could, with little danger of detection, sabotage an otherwise secure system. He described the state of the art of solving the "discrete logarithm" problem, and counselled the acceptance of a 1024-bit variable (agreed to by Smid), saying that a 512-bit variable provided only marginal security.

(U) Smid was the central speaker, and clearly felt himself to be under attack. He especially resented the implied slur on his character that the trapdoor insinuation represented, and allowed his sensitivity to prevent a balanced presentation.

(U) McCurley, sometimes a little too clever in making allusions to events or people who would be unfamiliar to much of the audience, made the valid point that DES and DSS have been the most challenged cryptosystems essentially because they were designed by the (untrustworthy!) U.S. government. He mentioned the "Biden Bill" (Senate bill 266) which, he said, authorized trapdoors in an effort to entrap drug dealers. He castigated a *Wall Street Journal* article, which had described the Lenstra attack as "potentially devastating," and Lenstra agreed that he had not used such language. McCurley displayed a 2-page cartoon (which he said had appeared in April, 1992 *Discover Magazine*) which badly distorted the facts of the case. I inferred from his words that he felt the cartoon had been inspired by RSA or by one their cronies.

(U) Desmedt referred to a letter written by Marty Hellman criticizing NIST. I had all but forgotten about Hellman; he has not been active on cryptologic scene in many years, and I've always had doubts about his moral principles (by contrast, I regard Rivest as being above all this dirt). Desmedt (and several other speakers) mentioned that trapdoors are a more severe problem for RSA than for the chosen DSS.

(U) Odlyzko, always a stimulating speaker and deep thinker, described trapdoors as a "minor distraction" and the risk due to trapdoors as "insignificant" relative to the importance of an extended key length. He regards 512 bits as "do-able in a couple of years," 768 bits as "do-

able in maybe 10 years" and 1024 bits as "maybe not out of reach." He gave an assessment of the importance of enhanced computational power (increased by about $10^3$ to $10^4$ over the past 15 years: we could factor 38- to 45-digit numbers in 1977, 115- to 129-digit numbers now) relative to algorithmic improvements, and described that proportion as "typical."

(U) Landrock seems to have missed the importance of the moment. He insisted on talking of some of his own research and overstated its importance to factoring and to trapdoors.

~~(C)~~ Jim Bidzos, the aggressive RSA representative, was unable to attend, but curmudgeon Whit Diffie presented a frail RSA position (Bidzos would have much more implacable) and was essentially ignored by the panel. Jim Massey pressed Smid gently on why RSA, described (by RSA, but also by others as well, and not without good reason) as a *de facto* standard, had not been selected. I think everyone understood that financial motives weighed heavily in the decision and in the subsequent quarrels. Apparently the patent issue even now has not been resolved. One wonders about the motives (and probability of success) of the appellants. Stuart Haber of Bellcore asked how NIST would skirt the exportability difficulty. The response was that any algorithm designed principally for encryption will probably run afoul of the State Department's restriction, while an algorithm deemed to apply to authentication need meet only Commerce's more lenient standards.

(U) A few other question were asked by the audience, but they were either innocuous or too technical to be included this informal trip report.

(U) Tuesday's night's rump session, as always, was a mixed bag. The chairman was Laszlo Csirmaz of Budapest, who is unknown to me. In fact, none of the Hungarians present made any impact on the technical side, nor do I remember them for their past contribution (except Nemetz, who is not yet a cryptologist). I attended only the first 10 (of 12) talks, wandering off to bed at 10:30.

(U) Kenji Koyama of NTT presented "Secure conference-key distribution schemes for conspiracy attacks." Koyama's proposal surfaced first at Eurocrypt '88. At Asiacrypt '91 a "conspiratorial attack" (by Shimbo and Kawamura), in which two or more users conspire to overcome security efforts, sent Koyama back to the drawing board. He has now announced a modest modification.

(U) Rafi Heiman returned with "A note on discrete logarithms with special structure." He has an interesting goal: suppose that we know that the elements whose logarithms we need to able to find satisfy some special condition (such as a small Hamming weight). Can an algorithm be found which has time on the order of the square root? Heiman has been unsuccessful, and ultimately this problem is unlikely to contribute much, but it would be a significant achievement if it could be resolved in the affirmative (or in the negative!)

(U) Ueli Maurer, who at a very tender age has established himself as a major contributor (he's one of Massey's students, and is still at ETH Zurich), spoke on noninteractive key-distribution systems. I couldn't see that he had must to say, but he said it very well. Nine minutes is not much time to present a talk, but his sentences contain much more than most.

(U) Another talk with an excellent speaker was "Implementation of an elliptic curve cryptosystem," presented by Canadian Gordon Agnew, representing joint work with Ron Mullin and Scott Vanstone, all of Waterloo. He described their implementation of discrete exponentiation in GF ($2^{593}$). Their most recent effort involved an optimal normal basis structure in GF ($2^{155}$). I don't have enough computer science knowledge to assess their progress, but I report to you that they utilized a limited instruction set and fewer than 11,000 gates. They attain a 40MHz clock speed and, using a Motorola 68030, they claim a throughput of 60 Kbps implemented on less than 1 square mil (less than 4% of the area of a smart card).

(U) Ivan Damgård and Li-dong Chen (she is a student of Landrock at Århus, where Damgård also works) presented "Security bounds for parallel versions of ID protocols." Fortunato Pesarin (of the statistics department at Palermo) laid the biggest egg with "On randomized cipher systems," but countryman Andrea Sgarro (an information theorist at Trieste) did better with "Information-theoretic bounds for authentication codes."

(U) Peter Mathys (he's either Swiss or Austrian, but he's been at Colorado for quite a while) presented "A fast serial encryption algorithm based on random transpositions," and Belgrade's Golic gave another reasonable performance with "A generalized correlation attack with a probabilistic constrained edit distance" (an improvement, he says, on the constrained Levenstein distance, if you know what that is).

(U) There was another talk, by Keiichi Iwamura, but it seemed to be a subset of the talk he was to give the following day, so we now turn to that program, devoted to public-key cryptosystems. Iwamura is at the Canon Research Center and is working with the very productive duo of Tsutomo Matusmoto and Hideki Imai of Yokohama University. He is interested in a speedy implementation of the RSA scheme, and has seized upon systolic arrays to implement modular multiplication. He says that for a 512-bit exponent $e$ and a 512-bit modulus $N$ they can achieve 50Kbps with about 25K gates.

(U) The other two talks in this session also dealt with efficiency. Yacov Yacobi of Bellcore (his coauthor is colleague Michael Beller) is interested in batch processing, and found that Batch-RSA cannot be employed effectively. He was happier with his efforts to apply batch processing in a Diffie-Hellman scenario, and the result was "Batch Diffie-Hellman key agreement systems and their application to portable communications," which uses composite moduli. Unfortunately one of the audience pointed out a flaw in one of his proofs; he made a hand-waving recovery, but the blunder had been clearly established.

(U) Kevin McCurley and his Sandia colleagues Ernie Brickell, Dan Gordon (now at the University of Georgia), and David Wilson (now at MIT) have been optimizing the exponentiation operation, both in conventional groups and in elliptic curve groups ("Fast exponentiation with precomputation"). Again, this subject is of undoubted importance (though it is perhaps not worth squeezing out the last epsilon, except to him who does it) and this is a powerful team which can be trusted to do the job well. I guess we as cryptologists should be happy to have such tasks carried out for us, freeing us to think of our own problems.

(U) The next four sessions were given over to philosophical matters. Complexity theorists are quite happy to define concepts and then to discuss them even though they have no examples of them. Jacques Patarin (Bull, France) wrestled with several of these at once in "How to construct pseudorandom and super-pseudorandom permutations from one single pseudorandom function," and, for those who needed another dose, one could listen to Babek Sadeghiyan (a student of Josef Pieprzyk at the University of New South Wales, Australia) discuss "Construction for super-pseudorandom permutations from a single pseudorandom function," but the next time I have the option, I will find something else to do.

(U) Ueli Maurer (ETH, Zurich), in "A simplified generalized treatment of Luby-Rackoff pseudorandom permutation generators," tried to persuade the philosophers that information theory may have something to say about their concerns. Maurer is remarkably versatile, and seems to be able to contribute substantially in several areas.

(U) Don Beaver (Penn State), in another era, would have been a spellbinding charismatic preacher; young, dashing (he still wears a pony-tail), self-confident and glib, he has captured from Silvio Micali the leadership of the philosophic wing of the U.S. East Coast cryptanalytic community. The subtitle tells it all in "how to break a 'secure' oblivious transfer protocol (or, good definitions mean everything)," in which he patched a tiny hole in a protocol of Bert den Boer which appeared at last year's Eurocrypt.

(U) Beaver collaborated with Stuart Haber (Bellcore) to produce "Cryptographic protocols probably secure against dynamic adversaries." Haber gave this talk, but it was not his finest hour. In past talks, he has injected some welcome humor, but this year he just preached the gospel, even though he conceded that what they were doing had also been done a few years ago by an MIT graduate student named Feldman, but that they "didn't like Feldman's definitions."

(U) The other talk in the first complexity-theory session was "Uniform results in polynomial-time security" given by the very young Paul Barbaroux (University of Paris). He found time to present only about one-third of his talk, which was probably just as well.

(U) Those of you who know my prejudice against the "zero-knowledge" wing of the philosophical camp will be surprised to hear that I enjoyed the three talks of the session better than any of that ilk that I had previously endured. The reason is simple: I took along some interesting reading material and ignored the speakers. That technique served to advantage again for three more snoozers, Thursday's "digital signature and electronic cash" session, but the final session, also on complexity theory, provided some sensible listening.

(U) The first talk, "Local randomness in candidate one-way functions," was by the amazing Austrian Harald Niederreiter (Austrian Academy of Science), representing work done jointly with Claus Schnorr (University of Frankfurt). Niederreiter writes beautifully and lectures beautifully too. I quote from their paper "A major open problem in cryptography is to establish one-way functions. While we cannot prove

one-wayness" [neither can anyone else—rek] "it makes sense to analyze candidate one-way functions and to prove properties of these functions that are useful in cryptographic applications." You might think this statement would be obvious to all, but in most cases, complexity theorists have never concerned themselves with actually finding a one-way function! Niederreiter also distanced himself from contemporary complexity theory by announcing that his results would depend on no unproved hypotheses.

(U) Now I cannot tell you that the veil has been lifted, and that one-way functions are finally fully (or even partially) understood. But it is refreshing to find a complexity theory talk which actually addresses an important problem! For this special occasion, I would really like to tell you what I think he said, but unfortunately it would require a string of definitions just to get to the statement of the two main results. Over $Z_N$ he takes m linearly independent (modulo the linear polynomials) polynomials $f_1, f_2, \ldots, f_m$ and maps the integer $x$ in $Z_N$ to the $m$-tuple formed from the least significant bit from each of the functions. He proposes such a function as a candidate one-way function. And of course there is the prospect of taking more than one least significant bit from each of the functions. How easy are these functions to invert?

(U) The other two talks again avoided anything of substance. Tatsuaki Okamoto of NTT (joint authors, Koichi Sakurai of Mutsubishi and Hiroki Shizuya of Tohomu University), in "How intractable is the discrete logarithm for a general finite group?" thought it worthwhile, in dealing the general discrete logarithm problem, to prove that the problem is contained in the complexity classes NP and co-AM, but is unlikely to be in co-NP.

(U) And Ueli Maurer, again dazzling us with his brilliance, felt compelled, in "Factoring with an Oracle" to arm himself with an Oracle (essentially an Omniscient Being that complexity theorists like to turn to when they can't solve a problem) while factoring. He's calculating the time it would take him (and his Friend) to factor, and would like also to demonstrate his independence by consulting his Partner as seldom as possible. The next time you find yourself similarly equipped, you will perhaps want to refer to his paper.

(U) The conference again offered an interesting view into the thought processes of the world's leading "cryptologists." It is indeed remarkable how far the Agency has strayed from the True Path.

(U) Hungary is a beautiful country that has freed itself from an oppressive occupation which lasted almost 45 years. From a tourist brochure: "Hungarians are now diligently learning English and German and are even more diligently forgetting Russian." The people sport American T-shirts but speak little English; they expect tourists to converse in German. Balatonfured is in a resort area around the region's largest lake (Lake Balaton). Accommodations are generally better, and prices higher, than elsewhere in the country. My Hungarian-American wife Donna and I spent three weeks in the country and experienced really wonderful weather: sunshine every day, cool nights (no need for air conditioning!). Twenty per cent of the 10 million people live in Budapest, but the next largest city is only one-tenth as large. The economy is basically agrarian; we observed extensive cultivation in virtually all of the countryside outside of the capital.

# An Agnostic Look at TQM


*William M. Nolte, P054*

Management techniques are like a tool box. The box does not contain a single magic tool for every job, but an assortment of tools that need to be selected according to the job at hand.

Total Quality Management can be an effective set of tools, offering impressive strengths: focus on the customer, empowerment of employees, action based on information, and continued improvement of processes. These strengths have led many organizations to adopt TQM techniques; some have gone even further and embraced the cult or religion of TQM. Despite my respect for the potential value of TQM—truth be told—I am a nonbeliever, a management school agnostic. NSA as an institution, however, has become a TQM believer, born again in the gospel of Deming. Actually, given the Agency's past enthusiasm for other management philosophies over the years, NSA can perhaps best be described as born again—and again—and again.

Is TQM a useful tool? Absolutely, but only if we recognize its weaknesses—even the risks—its incorporation entails for NSA. If we fail to do so, TQM not only will fail to improve the agency's operational performance, it will hamper a critical agency's ability to adapt to a difficult set of changed operating circumstances and encourage a the cynicism that will erode the morale of the agency's workforce.

## The Private Sector-Public Sector Gap

First of all, we must recognize that TQM, like most management schemes, derives from a private-sector experience. Such schemes inevitably translate only roughly into the public sector. For example, TQM's focus on the customer is essential for an organization that sometimes judges its success by internal measurement: that is, we think we do a good job, so we must be doing a good job. But what is the external measure for a public-sector organization? Private-sector organizations ultimately cannot judge their own success or failure. The market performs this function, except of course where a business is a monopoly or near monopoly. Utilities and regulated industries can evade the market, but look out if they lose their monopolistic or regulated niche. We will suffer, as public-sector organizations always do, from the absence of analogous measures for judging success or failure.

Even in the private sector, market circumstances can cloud or at least delay a true measure of success or failure. The American automobile industry represented, before the Japanese onslaught, something of a collective monopoly, with a virtually closed market and start-up costs too enormous to invite new players into the game. GM, Ford, and Chrysler (all their advertising notwith-

standing) barely competed with each other, as historically stable market shares would demonstrate. In this environment, a true measure of performance (and quality) was difficult to maintain. With the introduction of enormous numbers of Japanese cars, cheap, reliable, and efficient, the true measure of Detroit's inefficiency was apparent. Chrysler almost died, while GM and Ford recorded truly impressive losses.

P.L. 86-36

As a virtual monopoly, NSA has been largely spared the cost of inadequate support to its customers or lapses in quality of service rendered. We have been permitted to measure success in internal terms:

Most perversely, NSA, like other public sector organizations, has measured its success not in profit or productivity but in expenditure. The bigger the budget, the more successful the agency.

**The Factory**

The second risk associated with TQM is that it adopts an industrial metaphor. This is especially unfortunate for NSA which has traditionally been burdened with such a metaphor. After all, we produce "product"—not information, not a service, but product. Or at least that's what we've always said.

Wrong. We're in the service business, the information service business, to be exact, and one of the first things we need to do to remind ourselves of this is to drop all references to "product."

What's wrong with the product metaphor? Mostly that it confuses the measure of success. For years, we have graded our performance, at least in part, on the basis of how much product we have produced. If the number of product sections rose, we must be doing well.

Now, production statistics are useful in the private sector because they have a strong, though not unerring, correlation with efficiency and market savvy. If you're producing more product, customers must be demanding and buying more product. But the connection between demand and production is hazy at best in the public sector. (And even in the socialized private sector. Admiral Arleigh Burke used to tell of visiting a UK subsidiary of an American auto firm. Outside each plant, Burke was horrified to see acres and acres of cars. "How are you going to sell those cars?" Burke would ask, only to be told that selling them was less important than making them. The government, anxious to maintain employment levels, would reimburse the company for unsellable cars. This attitude has been satirized in the British comedy "Yes, Minister;" a bureaucrat rebukes his minister for demanding results: "We do not measure success by *results*, but by *activity*.")

We need to concern ourselves with satisfying our customers' needs for information. In some cases, those needs may require more reports. In others, the volume of reports may overwhelm the customer; then, the proper service might entail fewer reports. The point is we need to disconnect quality of service from number of (ugh!) products. They are only roughly related, if at all.

While we're on the subject of jargon, we need to take a look at the tendency to speak of customers' "requirements" rather than "needs." We give the customer the product they (say they) require. We must work on developing mechanisms to give them with the information they need, even if that means anticipating the customer's sense of those needs.

**"Getting it Right the First Time"**

Another unfortunate industrial memory from TQM is this business about "getting it right the first time." True and appropriate for GM—once they've entered production. But what a lousy idea this is for an organization that needs to tailor its service to an amazing range of customers whose needs will change dramatically and unpredictably as the world changes.

TQM seems to be best employed as an explicit strategy by companies operating in a relatively static environment and confronting significant repetitive precision, i.e., industrial quality, problems. It seems less attractive to firms that have to adjust to developing realities or, even more, operating in environments so fluid it makes no sense to even think about getting it right the first time. They may not even know what "it" is. When was the last time you saw Bill Gates of Microsoft emoting about how he has caught the TQM spirit? More likely, one is likely to watch Robert Stempel, former head of GM, talking about his commitment to the concept. Bill Gates has made billions for himself, created thousands of jobs, and enriched his stockholders. Stempel made millions for himself while disemploying thousands of workers and costing his stockholders billions. Now there's quality!

An emphasis on getting it right the first time also appears to contradict the TQM premises of continuing process improvement and eliminating fear from the

workplace. In the first instance, the very idea of process seems to contradict the stasis implicit in getting it right every time. Secondly, getting it right every time seems to assume that one is dealing with variables that will react with uniform predictability to the imposition of a given procedure. Shaping body panels probably reduces itself to this; dealing with people does not.

**At the Master's Feet**

(or Other Obsequious Positions)

Much of the TQM mythology leans heavily on a gross misreading of the career of the late W. Edwards Deming. Deming: the man who rebuilt Japan while his own country shamefully ignored him!

First of all, Deming did not rebuild Japan, the Japanese did—aided by the generosity of the United States. In the intricate matrix of ethic, skill, and capital that together encourage industrialism, the easiest component to replace is capital. It is also the one that requires the most frequent replacement. A skilled people, a work ethic intensified by the hardship of war, defeat, and occupation, and a rebuilt physical plant after about 1960 virtually guaranteed Japan some measure of success. Did Deming play a role? Yes, but he largely reinforced existing ethical and cultural tendencies. He did not supply them, a fact made clear by comparing Japan's post-1945 economic success with that of West Germany.

West Germany confronted the same basic situation facing Japan, a skilled people with a strong achievement ethic, confronted by lack of capital and the destruction of much of the country's physical plant. Like Japan, and in very similar time, Germany overcame its difficulties to become a great economic power—despite, miracle of miracles, the absence of Edwards Deming. Without question, Deming was useful to the Japanese and his role cannot be ignored. But Japan's economic emergence (really a continuation of a process that had begun in the 19th Century, only to be interrupted by the blunders of Japan's military leadership in the 1930s and 1940s) would have taken place without him.

Most importantly, the great danger of the myth of Deming is that it contributes to the overselling of TQM, especially through the evangelical quality of the sales pitch sometimes employed. One of the films being shown to agency TQM classes is a classic of the genre. A breathless "journalist," so thrilled to merely be in the presence of Dr. Deming she can barely speak, recounts that thousands of executives "have taken Deming to heart," caught his spirit, or otherwise experienced some sort of conversion. Companies of course must be "totally committed" to TQM for it to work, explaining why, despite Mr. Stempel's best efforts, GM did not turn around faster: Mr. Goodwrench didn't feel the spirit.

Deming was a fascinating man, especially for his often subtle, often overt fascination with the spiritual aspects of work. He believed, for example, that the job of a manager is to see that employees take joy in their work. A challenging concept? Yes. An admirable one? Probably. But the concept of joy is so subjective and the sources of joy so diverse and ultimately individual, that one could argue that it is something management cannot ultimately provide. Maybe all a job can do is offer the rewards—psychic and material—that permit individuals to pursue joy in the rest of their lives.

**The Fallacy of Total Commitment**

One of the problems with TQM as faith is embodied in the repetition of the mantra "total commitment." Faith indeed demands a total commitment. One can't believe in just nine commandments; faith in two parts of the trinity won't cut it; and the idea that there is probably only one God and Mohammed is one of several, equally valid messengers is not going to light the fires. Faith is an all-or-nothing proposition. You believe or you don't believe. Or you remain agnostic.

If this is the case, what are the Deming disciples to make of his contention that good ideas virtually never come from within an organization? If it's part of the dogma, we are at great pains to accept it. But for an agency like NSA, rightly if sometimes obsessively closed to the outside, this particular doctrine means we are in big trouble. We get only one truly significant outsider into the place every three years or so, with a relatively small, vitally important, but still insufficient infusion of outsiders from the military services. Do we believe Deming? Or do we conclude, on this and other issue, that Deming is valuable but not infallible?

If we accept the latter, we need move away from preaching TQM to teaching TQM, and that means teaching it warts and all. Management is not a faith process. It is not ideology. It is a technique: eclectic, applied, and particular. It is eclectic in that many tools exist for many different tasks. It is applied in much the way the late Ronald Lewin said wartime intelligence needed to be judged by its application: "The battle is the payoff." In management, performance is the payoff and the choice of tools is often secondary and sometimes academic.

Management is particular in that management experiences transfer only imperfectly from one organization to another. What works for Marriott may fail miserably for General Dynamics.

***By all means, let us use TQM.*** Let us put the customers first, where they should have been all along. Let us empower our employees. Let us develop (and use) measures for judging programs and supporting decisions. And finally, let us make continuous improvement of our processes an agency-wide commitment. ***But let's stop worshipping a screwdriver.*** That's not even good religion; it's idolatry. Rather than demanding total commitment, effective management requires a constant skepticism. Is the tool working? Is it the right tool?

Ultimately, managers must be prepared to admit they have been using the wrong tool and employ another—without fearing that they will be accused of heresy or infidelity. Here we cross from management to leadership, recalling what the late Grace Hopper said: "You don't manage people. You manage things. You lead people." And NSA, like other organizations is, in the words of another famous management authority, simply a collection of people—period!

**Quality management** is an effective interim goal for NSA; but our real objective must be **quality leadership**, consistent with our claim to be the world's leader in cryptology. TQM, of its own, will not produce this objective.

---

P.L. 86-36

## Technical Literature Report

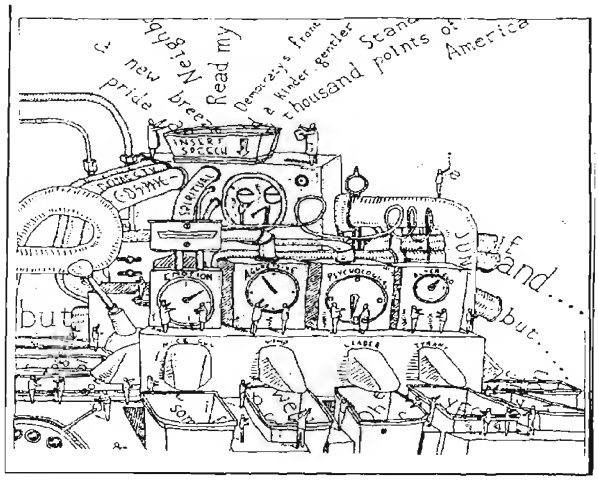
By [redacted] Z03

If you're looking for good articles on leadership, you can find one in (of all places!) the August 1992 issue of *Computer Language* magazine. The author, Larry Constantine, describes an interesting British study with some provocative results.

It seems that a British staff college was conducting a study of leadership in high achievers, so it assembled a large group of candidates and tested them for individual achievement. The candidates were sorted by achievement level, then regrouped. The new groups were tested again and regrouped a second time. The final groups ranged from "the best of the best" to "the worst of the worst." The groups were then assigned a collective task, with each one to be graded on its achievement as a group.

The results were not what the researchers expected. The group achievements bore little relationship to the individual achievements of the groups members. In fact, the "best of the best" group did much worse than "the worst of the worst." The immediate question was "What could possibly have happened?"

On reflection, the answer was simple. The initial tests had selected the "best" from the "worst" based on individual achievement; the "high achiever" selectees had focus, energy, drive, and the ability to get things done by themselves. But the final test was based on group achievement, and the groups of "high" achievers didn't show as much creativity, flexibility, and co-operation—as groups—as the groups of "low" achievers.




In fact, in one critical respect, the "lower" groups had a mix of leadership. Some of the members were *drivers* (although weaker ones than were found in the higher groups), but others were *innovators* (leaders in thinking of new ideas), *facilitators* (leaders in resolving conflicts between other members), and *implementers* (leaders in doing the dirty work), among others. While none of these "other leaders" was as effective—as individuals—as the members of the "higher" groups, the "lower" groups had people with leadership strengths in each of the specific problem areas they faced, so their group performance was better overall.

The lesson is clear. To build a high-achieving group, we need to look for—and appreciate—people who are different from ourselves. They may well not be classic individual "high achievers"—in fact, picking all uniformly "high achievers" may be the quickest way to disaster. Instead, we need to pick a mix of people, each of whom bring different strengths to complement each other's weaknesses and can work together to build the strongest team overall.

CRYPTOLOG
March 1994

*In commemoration of World War II, 1941-1945*

# Principles for Successful Guidance

*The Congressional Joint Committee on the Investigation of the Pearl Harbor Attack, after its thorough investigation of the attack, reached the conclusion that certain supervisory, administrative, and organizational deficiencies existed in the armed forces of the United States and recommended that serious consideration be given by the Army and Navy to twenty-five principles which it enunciated in the hope that something constructive might be accomplished that would aid our national defense and preclude a repetition of the failure of 7 December 1941. The twenty-five principles presented by the congressional committee are set forth below.*

I. Operational and intelligence work requires centralization of authority and clear-cut allocation of responsibility.

II. Supervisory official cannot safely take anything for granted in the alerting of subordinates.

III. Any doubt as to whether outposts should be given information should always be resoived in favor of supplying the information.

IV. The delegation of authority or issuance or orders entails the duty of inspection to determine that the official mandate is properly exercised.

V. The implementation of official orders must be followed with closest supervision.

VI. The maintenance of alertness to responsibility must be insured through repetition.

VII. Complacency and procrastination are out of place where sudden and decisive action is of the essence.

VIII. The coordination and proper evaluation of intelligence in time of stress must be insured by continuity of service and centralization of responsibility in competent officials.

IX. The unapproachable and superior attitude of officials is fatal: There should never be any hesitancy in asking for clarification of instructions or in seeking advice on matters that are in doubt.

X. There is no substitute for imagination and resourcefulness on the part of supervisory and intelligence officials.

XI. Communications must be characterized by clarity, forthrightness, and appropriateness.

XII. There is great danger in careless paraphrase of information received and every effort should be made to insure that the paraphrased material reflects the true meaning and significance of the original.

XIII. Procedures must be sufficiently flexible to meet the exigencies of unusual situations.

XIV. Restriction of highly confidential information to a minimum number of officials, while often necessary, should not be carried to the point of prejudicing the work of the organization.

XV. There is great danger of being blinded by the self-evident.

XVI. Officials should at all times give subordinates the benefit of significant information.

XVII. An official who neglects to familiarize himself in detail with his organization should forfeit his responsibility.

XVIII. Failure can be avoided in the long run only by preparation for any eventuality.

XVIX. Officials, on a personal basis, should never countermand an official instruction. Personal and official jealousy will wreck any organization.

XXI. Personal friendship, without more, should never be accepted in lieu of liaison or confused therewith where the latter is necessary to the proper functioning of two or more agencies.

XXII. No consideration should be permitted as excuse for failure to perform a fundamental task.

XXIII. Superiors must at all times keep their subordinates adequately informed, and conversely, subordinates should keep their superiors informed.

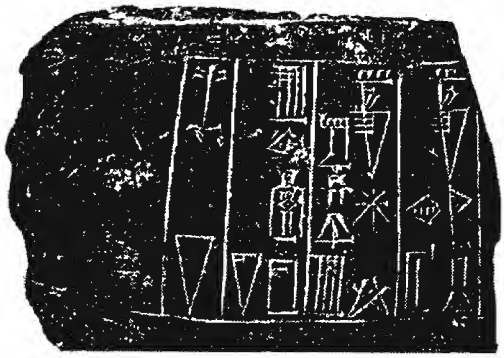
XXIV. The administrative organization of any establishment must be designed to locate failures and to assess responsibility.

XXV. In a well-balanced organization there is close correlation of responsibility and authority.

# *Lexicography at Second Hand:*

## Thoughts on Producing an "Exotic Language" Glossary

A631



~~(S-CCO) The~~ former Division of Languages and Linguistics (P16) was sometimes charged with creating an "exotic language"-English glossary, by translating the common side of an "exotic language"-common language glossary. An example is translating the Chinese side (the common side) of a Wa-Chinese glossary to produce a Wa-English glossary. Wa is of interest because it is spoken by a small group of people active in the drug trade who live in Southeast China and the adjacent area of Burma.

(U) This method of producing a glossary requires much less time and fewer resources than does the production of such a glossary from scratch—but it does have some pitfalls. In this case, for instance, the Chinese team that gathered the Wa vocabulary and wrote the glosses and explanations was based in Yunnan province. The local Yunnanese names for many of the common plants and wild animals do not exist in any published Standard Chinese dictionary. Sometimes, the Standard Chinese and Yunnanese gloss for the same character had different meanings—leaving me, the translator of the Chinese, groping for a proper gloss. The Chinese editor must have been a little near-sighted also, as some of the characters had elements that didn't fit the context, which gave me fits, unfamiliar as I was with the new orthography anyway.

(U) To make up for the difficulties encountered, I amused myself by reflecting on the life-style observed in explanations of some entries, and on things learned through them. In the Wa language, I ran across ideas that were expressed in unusual ways, that is, concepts that are foreign to someone whose first language is American English. For instance, the phrase accompanying the gloss for "hiccup" was, "Don't hiccup while eating; it will upset people." How does one hiccup? Thinking about the possibility of upsetting others by hiccuping while eating just might make one hiccup. And the phrase illustrating "going to bed" contains the passage, "lie nice and straight, don't curl up." What would prompt a parent to admonish a child with such a phrase? Is space so restricted in a Wa bed that curling up is a no-no?

(U) Going further afield one comes across the Wa words meaning "false leopard" which require the explanation that "false leopard" is a structure of bamboo over which the skin of the slain leopard is placed and used by the Wa to represent a leopard in a dance with religious significance performed after the hunt. A "blood mark" is made by a Wa hunter on the stock of his crossbow in the blood of the beast recently slain, to boast of the hunter's prowess with that weapon. An *ndo* is a "head pole"—a pole on which the severed head of an enemy is placed, while *nbing gaing* is the spot in a field where the pole is placed. (The Wa are said to have believed that placing a Han Chinese head at each of the four corners of a field would guarantee a good harvest.)

(U) At another level, the abundance of words relating to one area of life contrasted to the paucity of those relating to others can give an insight into the culture of a people. The Wa have common names for many things that they consider edible that the Western does not—many plants whose tender young leaves are edible—plants which we think of as only ornamental or regard as weeds. The glossary even lists an edible toad, unless the Chinese have mistakenly used the toad character to mean frog, which is highly unlikely. And what do we call the lump of flesh on the tail of a chicken? The Wa call it *beed*; it seems to be a logical thing to have named, since every chicken has one.

(U) The many grasses that are described as thatching material, and the descriptions of thatching methods and patterns, give an insight into what the typical Wa house might look like. One interesting pattern is said to look like sawteeth when seen from the inside of the structure.

(U) The consequences of careless behavior around a lac tree (a tree related to poison ivy on which the lac scale is parasitic) are brought out in the explanation that a child's hands are red and swollen because he was climbing and playing in a lac tree. The Wa word for "to carry in the mouth" is illustrated by the phrase, "the panther is carrying a piglet in its mouth." That, along with several other references to large carnivores, gives a little of the flavor of the Wa environment.

(U) Taken all together, I believe that the gains from a glance into another world more than make up for the difficulties met along the way.

DOCID: 4009689
CRYPTOLOG
March 1994

# Book Review

New Dictionary of English/Arabic Scientific and Technical Terms
by Ahmad Sh. Al-Khatib, 6th ed. 1991

*Reviewed by* [redacted] P.L. 86-36

(U) The New Dictionary Of Scientific and Technical Terms by Ahmad Sh. Al-Khatib is, in my opinion, one of the best technical reference aids that no Arabic linguist who must function in the scientific and technical Arabic language arena should be without. It is unmatched in breadth of technical terms as well as depth of any given term. The composition of the dictionary as well as the definitions and illustrations are based on western science and engineering concepts, which should prove the most beneficial to the educated Western reader/researcher. By and large, this dictionary provides definitions, but not encyclopedic descriptions of many of its terms. In some cases, the reader may have to use a more complete general Arabic/English Dictionary, such as the Hans Wehr, 4th ed., or the Al-Mawrid, to get the best meaning of a researched word.

(U) I've found that the definitions are mostly given in adherence to the true Arabic root, versus an English-sounding cognate, and the author as been as faithful as possible, when possible, to link newer concepts of science and engineering to traditional Arabic roots.

(U) The English used in this dictionary is more British English than American, but again, where possible, the author has taken care to give both the American and British term for the same Arabic word. For example, the Arabic word "miftah" can be found as the British term "spanner" and the American term "wrench"—under "S" and "W" respectively. Both of these definitions come with illustrations so the reader isn't necessarily thrown off by unfamiliar terms.

(U) In fact, there are illustrations (photos and drawings in both black-and-white and color) on almost every page. Some aren't as detailed when compared to the "Al-Mughni Al-Kabir" English/Arabic dictionary, but the collection in the "Sci/Tech Terms" is broader and quite satisfactory. Within the diagrammed illustration of an automobile, for instance, the reader will not see a steering wheel highlighted with both the English and Arabic word for it side by side, but will see the illustration with a brief description of what's being pictured on the margin in both English and Arabic.

(U) There are comprehensive tables in the back of the book which cover such items as the Geological Time Scale, equivalent Centigrade and Fahrenheit temperatures, the elements and their physical properties, and 4-place common logarithms, to name a few.

(U) There is one rather irritating problem that I discovered while searching for nuclear-related terms: pages 401-416 are missing. Page 400 ends with "Nitrogen Fixation" and page 417 begins with a chart on "Optics." I hope the problem is just with my copy and not with the entire pressing.

~~(FOUO)~~ In closing, let me say again that this dictionary, because of its depth and breadth of scientific and technical terminology and its adherence to traditional Arabic roots where possible, is a valuable linguistic asset to either the educated non-native English speaker, or the educated non-native Arabic speaker. We would do well to buy it.

## To the Editor:

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

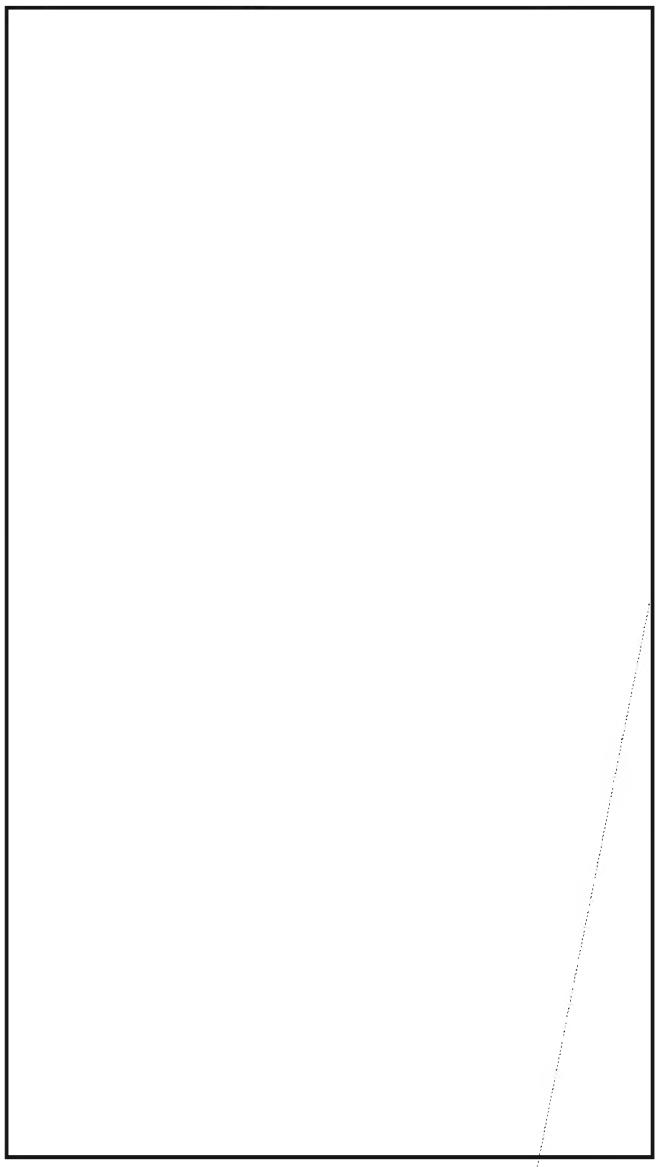
~~(C)~~ There was an interesting juxtaposition of articles in CRYPTOLOG's second issue of 1992, specifically [redacted] "Who Am I and What Am I Doing Here?" and [redacted] "On the Taxonomy of the Oyster." [redacted] discussed the definitions of bookbreaking and cryptolinguistics and the question of how to ensure fair recognition of those who are firmly planted in a hybrid of two demanding disciplines, while [redacted] differentiated between conventional substitution cryptosystems and codes.

~~(C)~~ In drawing the distinction between substitution and code systems, [redacted] touched upon a significant aspect of [redacted] question. Codes have traditionally been lumped among substitution systems by process of elimination, since they clearly do not fall into the transposition family. The shortcoming in this, however, is that it ignores a fundamental difference in the purposes of codes and substitution schemes. A code is used to alter the appearance of a language, while the more conventional substitution systems are used to alter the appearance of words. While this may seem subtle, to a bookbreaker it is crucial.

[redacted]

[redacted]

~~SECRET SPOKE~~



~~(C)~~ There are thorny questions aplenty to address, among them being: What is to be the official definition of a cryptolinguist? What are the essential skills? How do we develop those skills? How do we measure them? How do we determining what constitutes "professional" competence? How do we encourage diversity? For that matter, do we encourage diversity? How can we identify tours that will enhance a cryptolinguist's career? How do we identify and recruit potential cryptolinguists? How do we keep them?

~~(C)~~ We need to recognize bookbreaking/cryptolinguistics as a discipline in its own right. Ms. Goodlin touched on an obstacle to this recognition when she referred to her linguist friends and colleagues considering her to be a cryppie while her cryptanalyst friends and colleagues considered her to be a linguist. This attitude is harmless enough in your immediate peers. I think it important, though, that we be aware of and respect the unique talents required, and appreciate that neither a strictly language board not a strictly cryptanalytic board is the appropriate vehicle to adequately address the development of this particular set of cross-disciplinarians.

Z422 P.L. 86-36

EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~

**Government Communications Headquarters**
Room No E.0603
Priors Road Cheltenham GL52 5AJ
Telephone Cheltenham (0242) 221491 ext 2512
GTN Number 1366 ext 2512

P.L. 86-36

[redacted]
Editrix
CRYPTOLOG
c/o PO541,
NSA
[redacted]

Your reference
[redacted]
Date
2 July 1993

EO 1.4.(d)
P.L. 86-36

Dear Virginia,

**CRYPTOLOG 3RD ISSUE 1992**

May I please make two points about the article by Lambros Callimahos "A History of cryptology"; as it happens both refer to page 28.

First, he states that "In 1525, The British lion begins four centuries of successful cryptanalysis". This gives the impression that the British effort may have stopped around 1925. Nothing could be further form the truth! As just about anyone in Z Group will surely testify, the fifth century of British cryptanalysis is in full swing and continues to be as effective as ever...

Second, nobody seems to know when or where this lecture was delivered: but Lambros says that Brigadier Tiltman was then in the middle of his fifth decade as a cryptanalyst. I can confirm that the Brig joined GC&CS (the precursor of GCHQ) on 1 August 1920, so this would date the lecture as mid-1960s.

I was privileged to hear Lambros lecture when I was an integree in A5 in the late 1960s, and on another day he gave a flute recital in the Friedman Auditorium. A remarkable man, indeed.

Sincerely,

[redacted]

EO 1.4.(d)
P.L. 86-36

# CRYPTOLOG

Editorial Policy:

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that it is accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer. Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

How to submit an article:

N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to call the CRYPTOLOG editor on 963-3123s.

Send a hard copy accompanied by a diskette (either 3.5" or 5.25") to the editor at P0541 in 2E062, Ops. 1, or send via e-mail to mebutle@p.nsa. For maximum efficiency (as far as possible within the limits of your word processor):

- do not type your article in capital letters
- do not double-space between lines
- but do double-space between paragraphs
- do not indent for a new paragraph
- classify all paragraphs
- do not format an HD diskette as DD or vice-versa
- label your diskette: identify hardware (operating system: DOS or UNIX), density of medium, and word processor
- put your name, organization, building and phone number on the diskette

CRYPTOLOG is published in FrameMaker on a Sun HPW. If you do not have access to FrameMaker, ASCII format is preferred.